IN THE CLAIMS:

1. (Previously presented) A method in a first server data processing system for responding to a denial of service attack from a client, the method comprising:

detecting an occurrence of the denial of service attack from the client in which credentials are presented to the first server data processing system by the client, wherein the denial of service attack comprises sending invalid credentials to a server to consume resources of the server;

responsive to detecting the occurrence of the denial of service attack, blocking connections from the client to the first server data processing system;

responsive to detecting the occurrence of the denial of service attack, replaying an instance of the denial of service attack to a second server data processing system; and

responsive to a failure of the instance of the denial of service attack on the second server data processing system, sending a command to the second server data processing system to block connections from the client.

2. (Original) The method of claim 1, wherein the replaying step comprises:

presenting the credentials to the second server data processing system.

3. (Original) The method of claim 2, wherein the failure of the instance occurs if the second server data processing system fails to accept the credentials.

4. (Original) The method of claim 1 further comprising:

repeating the replaying step and the sending step for a set of server data processing systems.

5. (Original) The method of claim 1, wherein the detecting step comprises:

receiving the credentials from the client;

determining whether the credentials are valid; and

responsive to the credentials being invalid credentials, determining whether the denial of service attack from the client is occurring in response to receiving the invalid credentials.

6. (Original) The method of claim 5, wherein the step of determining whether the denial of service attack from the client is occurring in response to receiving the invalid credentials includes:

determining whether a number of the invalid credentials received from the client has exceeded a threshold selected to trigger a presence of the denial of service attack.

7. (Original) The method of claim 1 further comprising:

responsive to receiving the command from another server data processing system, blocking connections from the client.

8. (Original) The method of claim 1, wherein the command includes an instance of the denial of service attack and wherein the method further comprises:

responsive to receiving the command from another server data processing system, replaying the instance of the denial of service attack to the second server data processing system; and

responsive to the failure of the instance of the denial of service attack on the second server data processing system, sending the command to the second server data processing system to block connections from the client.

9-23. (Canceled)